



LEGAL & POLICY

Privacy Policy

How MyOwn ISP collects, uses and protects your personal information

Applies to: myownisp.co.za and the MyOwn ISP Client Portal

1. Introduction

MyOwn ISP, a division of ATEC Systems & Technologies (Pty) Ltd ("MyOwn ISP", "we", "us" or "our") provides fibre-to-the-home and fibre-to-the-business internet connectivity, delivered over the underlying FibreNetworks infrastructure and other licensed Fibre Network Operators ("FNOs"), together with our client portal, billing, support and related services (collectively, the "Services").

This Privacy Policy explains what personal information we collect from you when you visit our website, apply for or use our Services, or log in to the MyOwn ISP Client Portal, why we collect it, how we use and protect it, who we share it with, and what rights you have. It should be read together with our POPI Policy, our Terms & Conditions, and our Refund & Cancellation Policy.

This Privacy Policy is issued in terms of the Protection of Personal Information Act 4 of 2013 ("POPIA").

2. Who we are

Company	MyOwn ISP, a division of ATEC Systems & Technologies (Pty) Ltd
Registration number	2005/013296/07
Physical / registered address	Boardwalk Phase 4 Office Park, Block 3, 1st Floor, 107 Haymeadow Street, Faerie Glen, Pretoria
Information Officer	Marijke van Zyl
Information Officer email	marijke@atec.co.za
General enquiries	helpdesk@myownisp.co.za / 0861 122 832

3. Personal information we collect

We collect personal information directly from you, automatically through your use of our Services, and occasionally from third parties (such as FibreNetworks or another FNO, credit bureaus, or a payment gateway). The categories we collect include:

3.1 Identification and contact information

- Full name, South African ID number or passport number, date of birth
 - Residential and/or business installation address, billing address
 - Email address, mobile and landline numbers

3.2 Account and contract information

- Client Portal username, password (stored in hashed/encrypted form), account number
- Service package, contract term, installation date, equipment issued (ONT/router serial numbers)
- Correspondence with our sales, support and billing teams, including call recordings and support tickets

3.3 Payment and billing information

- Billing history, invoices, amounts paid, and payment status
- Payment method details processed via our payment gateways — PayFast, Ozow, Netcash, Zapper, and card payments via Visa, Apple Pay and Samsung Pay. MyOwn ISP does not store your full card number, card verification value (CVV) or Apple Pay / Samsung Pay device credentials; these are captured, tokenised and processed directly by our PCI DSS-compliant payment gateway partners.

3.4 Network, usage and technical information

- Fibre line and network diagnostic data (e.g. ONT signal levels, uptime, fault logs) needed to provision and support your line
- IP addresses allocated to your connection, session start/stop times, and data volumes, to the extent required for network management, billing, fault-finding and legal compliance
- Device and browser information, cookies and similar technologies used on our website and Client Portal (see clause 8)

3.5 Information required by law

- Information collected for compliance with the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 ("RICA"), where applicable to the Services
- Know-your-client and credit-vetting information used to assess creditworthiness before activating an account

4. How and why we use your information

We process your personal information for the following purposes, each of which is linked to a lawful basis under POPIA (contract performance, legal obligation, legitimate interest, or your consent):

- **Providing the Service:** to assess your application, provision and install your fibre line, activate and maintain your connection, and provide technical support.
- **Billing and payment:** to generate invoices, process payments through our payment gateway partners, collect overdue amounts, and prevent fraud.
- **Client Portal:** to authenticate you, display your account, usage, billing and support information, and let you manage your Services online.
- **Communication:** to send service notifications, maintenance and outage alerts, invoices, and to respond to queries and complaints.

- **Direct marketing:** to send you information about offers, upgrades or new products, but only with your consent as required by section 69 of POPIA, and always with an easy opt-out on every communication.
- **Legal and regulatory compliance:** to comply with ICASA regulations, RICA, tax and consumer protection laws, and to respond to lawful requests from regulators or law enforcement.
- **Network integrity and security:** to monitor, secure and improve our network and the Client Portal, detect fraud, abuse or unlawful use, and enforce our Terms & Conditions.

5. Sharing and disclosure of your information

We do not sell your personal information. We share personal information only where necessary, and always subject to appropriate confidentiality and (where required) operator agreements as contemplated in POPIA:

- **FibreNetworks and other Fibre Network Operators (FNOs):** the wholesale network owner(s) over whose infrastructure your line runs receive the minimum information necessary (e.g. installation address, order and fault reference) to provision, activate, maintain and repair your physical fibre connection.
- **Payment gateways and financial institutions:** PayFast, Ozow, Netcash, Zapper, Visa, Apple Pay and Samsung Pay (and the banks underlying them) to process your payments securely.
- **Service providers acting on our behalf:** IT hosting and Client Portal software providers, billing and invoicing platforms, SMS/email notification providers, debt collection agencies, and credit bureaus, each under a written agreement requiring them to protect your information and use it only for the purpose we specify.
- **Regulators and law enforcement:** ICASA, the Information Regulator, the South African Revenue Service, and law enforcement or intelligence agencies, where we are legally required or permitted to disclose information (including under RICA).
 - **Professional advisors:** our auditors, attorneys and insurers, where reasonably necessary.
- **Business transfers:** a purchaser or prospective purchaser in the event of a sale, merger, or restructuring of MyOwn ISP's business, subject to confidentiality safeguards.

6. Cross-border transfers

Some of our service providers (for example, cloud hosting or payment processing infrastructure) may process personal information outside South Africa. Where this occurs, we ensure the recipient is subject to a law, binding corporate rules, or an agreement that provides an adequate level of protection substantially similar to POPIA, or that you have consented to the transfer, in accordance with section 72 of POPIA.

7. Data retention

We retain personal information only for as long as necessary to fulfil the purposes described in this Policy, including to satisfy any legal, accounting, regulatory (including ICASA and RICA) or reporting requirements. As a general rule:

- Account, billing and contract records are retained for the duration of your contract and for 5 years thereafter, in line with tax and consumer protection record-keeping obligations.
- Network and communication-related information collected under RICA is retained for the minimum period prescribed by that Act.
- Call recordings and support tickets are retained for 24 months for quality assurance and dispute-resolution purposes.
- Marketing consent records are retained until you withdraw consent, plus a reasonable period to give effect to that withdrawal.

Once retention periods expire, we securely delete, destroy or de-identify the information.

8. Cookies and similar technologies

Our website and Client Portal use cookies and similar technologies to keep you logged in, remember your preferences, understand how our site is used, and improve performance and security. These may include strictly necessary cookies (required for login and payment processing), functional cookies, and analytics cookies.

You can manage or disable non-essential cookies through your browser settings. Disabling strictly necessary cookies may prevent the Client Portal or payment gateways from functioning correctly.

9. Security of your information

We implement appropriate technical and organisational measures to protect personal information against loss, unauthorised access, alteration or disclosure, as required by Condition 7 (Security Safeguards) of POPIA. These measures include:

- Encryption of data in transit (TLS/SSL) on our website and Client Portal
- Access controls, role-based permissions and logging for staff access to client records
- Use of PCI DSS-compliant payment gateways so that MyOwn ISP never stores full card, Apple Pay or Samsung Pay credentials
- Regular review of our security measures and staff training on information security and confidentiality

No system is completely secure. If we become aware of a security compromise that has affected your personal information, we will notify the Information Regulator and you as required by section 22 of POPIA, as soon as reasonably possible after discovery.

10. Your rights

Subject to POPIA, you have the right to:

- Be informed that we hold personal information about you, and to access that information;
- Request correction, updating or deletion of personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully;
- Object, on reasonable grounds, to the processing of your personal information, including for direct marketing purposes;
- Withdraw any consent you have given, at any time (this does not affect processing carried out before withdrawal, or processing we are otherwise entitled or required to continue);
- Not be subject to a decision based solely on automated processing that affects you legally or significantly, without an opportunity to make representations;
- Lodge a complaint with the Information Regulator if you believe we have processed your personal information unlawfully.

To exercise any of these rights, contact our Information Officer using the details in clause 2. We may need to verify your identity before actioning a request, and will respond within the timeframes required by POPIA.

Information Regulator contact details

Website	www.inforegulator.org.za
Email (general enquiries)	infoereg@justice.gov.za
Email (POPIA complaints)	POPIAComplaints@inforegulator.org.za

11. Direct marketing

We will only send you direct marketing communications (SMS, email or telephone) if you have consented, or where permitted under the limited exception in section 69(3) of POPIA for existing customers regarding similar products or services, provided you are given a clear opportunity to opt out, free of charge, on each communication.

12. Children's information

Our Services are intended for account holders who are 18 years or older. We do not knowingly collect personal information from children other than as strictly necessary and with the consent of a competent person, as contemplated in section 35 of POPIA.

13. Changes to this Policy

We may update this Privacy Policy from time to time to reflect changes in our Services, technology, or legal requirements. The current version will always be available on our website and the Client Portal, together with its effective date. Material changes will be communicated to you via email or a notice on the Client Portal.

14. Contact us

If you have any questions about this Privacy Policy or how we handle your personal information, please contact our Information Officer using the details set out in clause 2 above.